South Dakota Department of Human Services

Policy Title:	Administrative, Technical, and Physical Safeguards Policy		
Policy Number:	**DHS-100-05**	**Version:**	1.0
Approved By:	**Betty Oldenkamp, DHS Secretary**		
Effective Date:	April 14, 2003		

Purpose:

The intent of this policy is to establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use or disclosure.

This document contains guidance for developing procedures to implement this policy.

Policy:

1. **General**

DHS must take reasonable steps to safeguard protected health information or PHI from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of PHI.

2. **Safeguarding PHI – DHS workplace practices**

a. Paper

i. Each DHS workplace will store files and documents containing PHI in locked rooms or storage systems.

ii. In workplaces where lockable storage is not available, DHS staff must take reasonable efforts to ensure the safeguarding of PHI.

iii. Each DHS workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

iv. Each DHS workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

a. Oral:

i. DHS staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs.

ii. Each DHS workplace shall make reasonable efforts to provide enclosed offices and/or interview rooms for the verbal exchange of PHI.

Exception: In work environments structured with few offices or closed rooms, such as at the Central Office in Pierre, or other open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that DHS has met the reasonable safeguards and minimum necessary requirements.

iii. Each DHS workplace must foster employee awareness of the potential for inadvertent verbal disclosure of PHI.

c. Visual:

i. DHS staff must ensure that observable PHI is adequately shielded from unauthorized disclosure on computer screens and paper documents.

A. Computer screens: Each DHS workplace must make every effort to ensure that PHI on computer screens is not visible to unauthorized persons.

B. Paper documents: DHS staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard PHI.

3. **Safeguarding PHI – DHS administrative safeguards**

a. Implementation of role-based access and **DHS Policy DHS-100-04,** "Minimum Necessary Information" will promote administrative safeguards.

i. Role Based Access (RBA) is a form of security allowing access to data based on job function in accordance with DHS security

procedures. Employees shall be assigned to an RBA group that will give members access only to the minimum necessary information to fulfill their job functions.

b. Conducting internal reviews periodically will permit DHS to evaluate the effectiveness of safeguards.

i. DHS Administrators and Directors or their designee will use the **DHS 2098 "**Safeguard Assessment Tool" and **DHS 2099 "**Guidance for Administrative, Technical and Physical Safeguards for Protected Health Information (PHI)" to conduct annual reviews in order to evaluate and improve the effectiveness of their current safeguards.

Guidance for Procedure Development:

The following guidelines should be used in developing procedures to implement this policy.

1. **General**

There are no accompanying procedures.

2. **Safeguarding PHI – DHS workplace practices**

a. Paper

i. Files and documents being stored:

A. Lockable desks, file rooms, open area storage systems must be locked.

B. Where DHS has desks, file rooms, or open area storage systems, that are not lockable, reasonable efforts to safeguard PHI must be implemented.

ii. Files and documents awaiting disposal/destruction:

A. Desk-site containers: The DHS workplace will ensure that PHI awaiting disposal is stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

B. Storage rooms containing PHI awaiting disposal: Each DHS workplace will ensure that storage rooms are locked after business hours or when authorized staff are not present.

C. Centralized waste/shred bins: Each DHS workplace will ensure that all centralized bins or containers for disposed of PHI are clearly labeled "confidential", sealed, and placed in a lockable storage room.

D. Each DHS workplace that does not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

iii. Shredding of files and documents consistent with record retention requirements:

A. DHS staff: Must ensure that shredding is done timely, preferably on a daily basis.

B. Outside contractors: DHS must ensure that such entity is under a written contract that requires safeguarding of PHI throughout the destruction process.

b. Oral

i. DHS staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs, and should be aware of risk levels.

A. Locations of verbal exchange with various risk levels:

I. Low risk: interview rooms, enclosed offices and conference rooms.

II. Medium risk: employee only areas, telephone and individual cubicles.

III. High risk: public areas, reception areas and shared cubicles housing multiple staff where clients/patients or participants are routinely present.

c. Visual:

i. DHS staff must ensure that observable PHI is adequately shielded from unauthorized disclosure.

Example: Information containing client/patient's PHI should be face down while laying in open view on the staff's desk during their workday and in the process of utilizing this PHI.

ii. Computer screens: DHS offices must ensure that PHI on computer screens is not visible to unauthorized persons. Suggested means for ensuring this protection include:

A. Use of polarized screens or other computer screen overlay devices that shield information on the screen from persons not the authorized user;

B. Placement of computers out of the visual range of persons other than the authorized user;

C. Clearing information from the screen when not actually being used;

D. Locking-down computer work stations when not in use; ***or***

E. Other effective means as available.

iii. Paper documents: DHS staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard PHI.

A. DHS staff must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper documents containing PHI that are located on:

I. Desks;

II. Fax machines;

III. Photocopy machines;

IV. Portable electronic devices (e.g., laptop computers, palm pilots, etc.);

V. Computer printers; ***and***

VI. Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

3. **Safeguarding PHI – DHS administrative safeguards**

    a. Role Based Access (RBA): Roles will be created and defined based on the information DHS owns and where it is located and how it is used and why. A determination of who should have access to the specific data will be established.

        i. DHS Administrators and Directors or their designee will decide the role of each of their staff and request exceptions based on the needs of their office.

        ii. DHS Administrators and Directors or their designee are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.

    b. DHS Administrators and Directors or their designee will:

        i. Follow the instructions given in **DHS 2099** "Guidance for Administrative, Technical and Physical Safeguards for PHI";

        ii. Conduct a thorough assessment by using **DHS 2098** "DHS Safeguard Assessment Tool";

        iii. Foster a more secure atmosphere and enhance the belief that PHI is important and that protecting privacy is key to achieving DHS goals; ***and***

        iv. Will update the safeguards in place each year, seeking to achieve reasonable administrative, technical and physical safeguards.

Reference(s):

- 45 CFR Part 164

Form(s):

- **DHS 2098** "Safeguard Assessment Tool"
- **DHS 2099** "Guidance for Administrative, Technical and Physical Safeguards for Protected Health Information (PHI)"

Contact(s):

- For Central Office Staff and Field Office Staff - DHS HIPAA Privacy Office, (605) 773-5990
- For Human Services Center Staff – DHS HIPAA Privacy Contact, (605) 668-3100
- For South Dakota Developmental Center Staff – DHS HIPAA Privacy Contact, (605) 472-2400